CLAIMS

1. A method comprising the steps of:

(a) generating hash data based on at least one of a universal resource locator (URL) of a resource, resource access right data defining restriction(s) on a web access device (WAD) and/or user thereof to access the resource, and an internet protocol (IP) address of the WAD; and

(b) combining the hash data, URL, and resource access right data in a web page.

2. A method as claimed in claim 1 further comprising the step of:

(c) transmitting the web page document including the secure URL to the WAD in response to a request for the web page document from the WAD.

3. A method as claimed in claim 1 wherein the hash data is further generated based on key data.

4. A method as claimed in claim 3 wherein steps (a) - (c) are performed at a resource provider subsystem (RDS), the method further comprising the step of:

(c) transmitting the key data from the RPS to a resource distribution subsystem (RDS) hosting the resource so that, if the secure URL is activated by the web access device to generate a request for the resource to the RDS, the RDS can verify that the resource access right data has not been modified other than by the RPS.

5. A method as claimed in claim 1 wherein the resource access right data includes at least one of:

1) an authorized Internet protocol (IP) address or IP address range;

2) lifespan data indicating the lifespan indicating a time period over which requests for accessing a resource are valid; and/or

3) maximum reference data indicating a maximum number of times a web access device and/or user thereof can access a resource.

6. A method comprising the steps of:

at a resource provider subsystem (RPS),

(a) receiving a request for a web page from a web access device via a network, the request including a network address of the web access device;

(b) determining resource access right data for the web access device and/or a user thereof, the resource access right data defining restriction(s) for the web access device and/or user thereof to access a resource;

(c) securing a universal resource locator (URL) for a resource by generating hash data based on at least one of the URL, a network address of the web access device, and/or resource access right data, and combining the URL, resource access right data, and hash data together in the web page; and

(d) transmitting the web page having the secure URL to the web access device via the network in response to the request received in step (a) from the web access device.

7. A method as claimed in claim 6 wherein the hash data is generated further using key data corresponding to the web access device and/or user thereof, the method further comprising the step of:

(e) transmitting key data corresponding to the web access device and/or user thereof to a resource distribution subsystem (RDS) hosting the resource so that, if the secure URL is activated by the web access device to generate a request for the resource to the RDS, the RDS can verify that the resource access right data has not been modified other than by the RPS.

8. A method as claimed in claim 6 wherein the network address of the web access device is an internet protocol (IP) address.

9. A method comprising the steps of:

(a) receiving a signal requesting a web page document from a web access device (WAD), the signal including an Internet protocol (IP) address of the WAD;

(b) retrieving data for the web page document including a universal resource locator (URL) of a document referenced in the web page document;

(c) retrieving resource access right data for the URL using the IP address of the web access device and/or user name and password established through a log-in procedure;

(d) generating hash and/or encrypted data to generate secure resource access right data;

(e) combining the resource access right data with the respective URL to generate a secure URL; and

(f) generating the web page document including the secure URL; and

(g) transmitting the secure URL to the WAD.

10. A method comprising the step of:

at a web access device (WAD),

(a) transmitting a signal requesting a web page document to a resource provider subsystem (RPS); and

(b) receiving the web page document having a secure universal resource locator (URL) with hash data, URL, and resource access right data, in response to the request.

11. A method as claimed in claim 10 further comprising the step of:

(c) activating the secure URL with the WAD to transmit a signal requesting access to a resource designated by the URL to a resource distribution subsystem (RDS); and

(d) accessing the resource with the WAD if the RDS determines that access to the resource is authorized based on the hash data and resource access right data contained in the request signal.

12. A method comprising the steps of:

(a) at a web access device (WAD), generating and transmitting a request for a web page document to a resource provider subsystem (RPS);

(b) receiving the requested web page document having a secure universal resource locator (URL) with secured resource access right data from the resource provider subsystem (RPS);

(c) executing a browser application and web page document with the WAD to generate and transmit a signal to request a resource distribution subsystem (RDS) to provide access to a resource identified by the secure URL, the request signal including the URL and secure resource access right data; and

(d) if access to the resource is permitted by the RDS, accessing the resource with the WAD.

13. A method as claimed in claim 12 wherein the step (d) comprises the substeps of:

(d1) receiving at the WAD resource data from the RDS;

(d2) storing the resource data in memory of the WAD;

(d3) executing an application with the WAD based on the resource data to generate a signal; and

(d4) generating a display with the WAD based on the signal generated in the substep (d3).

14. A method as claimed in claim 12 wherein the step (d) comprises the substeps of:

(d1) receiving a program module resource from the RDS;

(d2) loading the program module resource into memory of the WAD;

(d3) executing the program module resource with the EAD to generate a signal;

(d4) storing the signal(s) in memory; and

(d5) generating a display with the WAD based on the signal generated in the substep (d4).

15. A method as claimed in claim 12 wherein the step (d) comprises the substeps of:

(d1) receiving at the WAD via the network a signal from the RDS generated based on execution of a server application by the RDS;

(d2) storing the received signal in the memory of the WAD;

(d3) generating with the WAD a display signal based on the signal received in the substep (d1);

(d4) generating a display with the WAD based on the display signal;

(d5) executing a client application with the WAD to generate a signal based on the signal from the RDS; and

(d6) transmitting the signal(s) to the RDS via the network.

16. A method as claimed in claim 12 further comprising the step of:

(d7) receiving input data at the WAD from a user, the client application executed in step (d5) based on the input data.

17. A method comprising the steps of:

at a resource distribution subsystem (RDS),

(a) receiving a signal requesting access to a resource from a web access device (WAD), the signal including at least a universal resource locator (URL), resource access right data, and hash data;

(b) verifying that the resource access right data as set by a resource provider subsystem (RPS) has not been changed, using the hash data;

(c) if the verifying establishes that the resource access right data has not been changed, determining whether access to the resource is permitted to the WAD and/or user thereof based on the resource access right data; and

(d) if the resource access right data indicates that the WAD and/or user thereof is authorized to access the resource, permitting access to the resource to the WAD and/or user thereof.

18. A method as claimed in claim 17 wherein the resource access right data includes at least one of:

1) an authorized Internet protocol (IP) address or IP address range;

2) lifespan data indicating the lifespan indicating a time period over which requests for accessing a resource are valid; and

3) maximum reference data indicating a maximum number of times a web access device and/or user thereof can access a resource.

19. A method as claimed in claim 17 wherein the hash data is generated based on the URL, resource access right data, and key data, the method further comprising the step of:

(e) receiving key data from the RPS for use in verifying in step (b) that the resource access right data has not changed from establishment by the RPS.

20. A method as claimed in claim 17 wherein the key data includes a key and optionally at least one of:

1) a second URL identifying the RPS;

2) start date/time data identifying a date and time at which a key is valid;

3) end date/time data identifying a date and time at which a key becomes invalid;

4) lifespan data indicating a period of time over which the key is valid;

5) key index data identifying the key from among a plurality of different keys;

6) hash identifier data indicating to the RDS a hash algorithm to be performed to generate the hash data;

7) encryption data indicating an encryption model and/or algorithm used to encrypt and decrypt resource access right data; and

8) format fields data indicating the number of fields in the signal requesting access to the resource.

21. A method comprising the steps of:

(a) receiving a signal requesting access to a resource, the signal having a secure universal resource locator (URL) with secured resource access right data;

(b) extracting an Internet protocol (IP) address from the secured resource access right data;

(c) comparing the extracted IP address with the IP address included in a hypertext transport protocol (HTTP) message of the request signal; and

(d) authenticating that the IP address of the secured resource access right data corresponds to the IP address of a device requesting access to the resource, based on the comparing of step (c).

22. A method as claimed in claim 21 further comprising the step of:

(e) terminating the request signal if the authenticating of step (d) indicates that the IP address of the secured resource access right data does not match the IP address extracted from the HTTP message.

23. A method as claimed in claim 22 further comprising the steps of:

(e) if the authenticating of step (d) indicates that the IP address of the secure resource access right data matches the IP address of the device requesting access to the resource, obtaining a key corresponding to the IP address;

(f) verifying whether the key is valid based on data corresponding to the key in a secure content key database;

(g) generating hash data based on at least the IP address, URL, and key; and

(h) verifying that the hash data generated in the step (g) matches the hash data included in the request signal received in the step (a).

24. A method as claimed in claim 23 further comprising the steps of:

(i) terminating the request signal if the verifying of the step (h) indicates that the hash data generated in the step (g) does not match the hash data included in the request signal received in the step (a).

25. A method as claimed in claim 23 further comprising the steps of:

(i) determining whether access to a resource is to be provided to a device identified by the IP address, based on the resource access right data included in the request signal;

(j) retrieving the resource based on the URL included within the request signal; and

(k) providing access to the resource to a device identified by the IP address if the determining of step (j) indicates that access to the resource is to be provided, based on the URL.

26. A method as claimed in claim 25 further comprising the steps of:

(l) retrieving resource access right data from a database,

the determining of step (j) based further on whether the IP address of the request signal is authorized to access the resource indicated by the URL of the request signal, based on the retrieved resource access right data.

27. A method as claimed in claim 26 further comprising the steps of:

(m) terminating the request signal if the determining of the step (l) indicates that access to the resource is not to be provided based on the resource access right data included in the request signal.

28. A method as claimed in claim 26 wherein the resource access right data retrieved in the step (k) includes maximum reference data and reference count data, the method further comprising the step of:

(n) incrementing the reference count data to indicate that access to the resource has been requested by the request signal;

(o) comparing the incremented reference count data with the maximum reference count data; and

(p) providing access to the resource if the comparing of step (o) indicates that the incremented reference count data does not exceed the maximum reference count data.

29. A method as claimed in claim 26 wherein the resource access right data retrieved in the step (k) includes lifespan data for access to the resource indicated by the URL, the method further comprising the steps of:

(m) determining a time and date of receiving the request signal in step (a);

(n) comparing the lifespan data with the time and date of receiving the requesting signal; and

(o) determining that the IP address of the request signal is authorized to access the resource, if the comparing of the step (n) indicates that the time and date of receiving the request signal is within the lifespan data.

30. A method as claimed in claim 29 wherein the resource access right data retrieved in the step (k) includes URL/resource provider identification data, the method further comprising the step of:

(p) retrieving the resource from a resource provider subsystem via the Internet, based on the URL/resource provider identification data, the retrieved resource used to provide access to the resource in the step (k).

31. A method as claimed in claim 30 wherein the resource access right data retrieved in the step (l) includes retrieval key data used to decrypt the resource retrieved in the step (p).

32. A method comprising the steps of:

(a) receiving a signal requesting access to a resource, the request signal including a universal resource locator (URL), secured resource access right data, and an Internet protocol (IP) address of a device requesting access to the resource, and hash data;

(b) verifying whether key data is valid based on data corresponding to the key data in a secure content key database;

(c) if the key data is verified as valid in step (b), generating hash data based on at least the IP address, URL, and the key data; and

(d) verifying that the hash data generated in the step (c) matches the hash data included in the request signal received in the step (a).

33. A method as claimed in claim 32 further comprising the steps of:

(e) terminating the request signal if the verifying of the step (d) indicates that the hash data generated in the step (c) does not match the hash data included in the request signal received in the step (a).

34. A method as claimed in claim 33 further comprising the steps of:

(f) determining whether access to a resource is to be provided to a device identified by the IP address, based on the resource access right data included in the request signal; and

(g) providing access to the resource to a device identified by the IP address if the determining of the step (f) indicates that access to the resource is to be provided.

35. A method as claimed in claim 34 further comprising the steps of:

(h) retrieving resource access right data from a database,

the determining of step (f) based further on whether the IP address of the request signal is authorized to access the resource indicated by the URL of the request signal, based on the retrieved resource access right data.

36. A method as claimed in claim 32 wherein the request signal received in step (a) includes key index data, the method further comprising the step of:

(e) retrieving the key data from the secure content key database using the key index data.

37. A method as claimed in claim 32 wherein the step (b) comprises the substeps of:

(b1) determining a date and time of receiving the request signal in the step (a);

(b2) retrieving start date/time data and end date/time date from a database;

(b3) comparing the date and time of the request signal with the start date/time data and end date/time data; and

(b4) determining whether the key data is valid, based on the comparing of the step (b3).

38. A method as claimed in claim 32 wherein the step (b) comprises the substeps of:

(b1) determining a date and time of receiving the request signal in the step (a);

(b2) retrieving lifespan data from a database;

(b3) comparing the date and time of receiving the request signal with the lifespan data; and

(b4) determining whether the key data is valid, based on the comparing of the step (b3).

39. A method comprising the steps of:

(a) receiving via the Internet a request signal including a universal resource locator (URL) indicating a location of a resource, secured resource access right data indicating rights of a device to access the resource, and an Internet protocol (IP) address of the device;

(b) determining whether access to the resource is to be provided to the device identified by the IP address, based on secured resource access right data included in the request signal; and

(c) providing access to the resource to a device identified by the IP address if the determining of the step (c) indicates that access to the resource is to be provided.

40. A method as claimed in claim 39 further comprising the step of:

(d) terminating the request signal if the determining of the step (b) indicates that access to the device is not authorized.

41. A method as claimed in claim 39 wherein said step (c) comprises the substep of transmitting the resource to the device via the Internet.

42. A method as claimed in claim 39 further comprising the step of:

(d) authenticating the request signal if an Internet protocol (IP) address of the URL in the request signal matches a URL of the device contained in the resource access right data of the request signal.

43. A method as claimed in claim 39 further comprising the steps of:

(d) retrieving resource access right data from a database,

the determining of step (b) based further on whether the IP address of the request signal is authorized to access the resource indicated by the URL of the request signal, based on the retrieved resource access right data.

44. A method as claimed in claim 39 further comprising the step of:

(d) verifying validity of key data;

(e) generating hash data based on at least the URL and the key data;

(f) comparing the hash data generated in step (e) with hash data included in the received request signal;

(g) determining whether the hash data generated in step (e) matches the hash data generated in the request signal, based on the comparing of the step (f),

the access to the resource provided in step (c) if the determining of step (g) establishes that the hash data match.

45. A method as claimed in claim 44 wherein the step (d) comprises the substeps of:

(d1) determining a date and time of receiving the request signal in the step (a);

(d2) retrieving start date/time data and end date/time date from a database;

(d3) comparing the date and time of the request signal with the start date/time data and end date/time data; and

(d4) determining whether key data is valid, based on the comparing of the step (b3),

steps (e) through (g) performed if the key data is determined to be valid and not otherwise.

46. A method as claimed in claim 44 wherein the step (d) comprises the substeps of:

(d1) determining a date and time of receiving the request signal in the step (a);

(d2) retrieving lifespan data from a database;

(d3) comparing the date and time of receiving the request signal with the lifespan data; and

(d4) determining whether key data is valid, based on the comparing of the step (b3),

steps (e) through (g) performed if the key data is determined to be valid and not otherwise.

47. A system using the Internet, the system comprising:

at least one web access device (WAD) executing a browser application, the WAD generating a signal requesting a web page document having a secure universal resource locator (URL), receiving the web page document having the secure URL, displaying the web page document having the secure URL, and generating a signal requesting a resource indicated by the secure URL of the web page document;

a resource provider subsystem (RPS) coupled to receive via the Internet the signal requesting the web page document from the WAD, the RPS generating the secure URL to include resource access right data defining restriction(s) of the WAD and/or user thereof to access the resource indicated by the URL, the RPS transmitting the web page document with the secure URL to the WAD; and

at least one resource distribution subsystem (RDS) coupled to receive via the Internet the signal from the WAD requesting access to the resource, the RDS determining whether the resource access right data has been changed from establishment by the RPS, and, if the RDS determines that the resource access right data has not been changed, the RDS determining whether the WAD and/or user thereof is authorized to access the resource using the resource access right data, the RDS permitting access to the resource if the WAD and/or user thereof is authorized to access the resource.

48. A system as claimed in claim 47 wherein the resource access right data includes at least one of:

1) an authorized Internet protocol (IP) address or IP address range;

2) lifespan data indicating the lifespan indicating a time period over which requests for accessing a resource are valid; and/or

3) maximum reference data indicating a maximum number of times a web access device and/or user thereof can access a resource.

49. A system as claimed in claim 47 wherein the hash data is generated by the RPS based on the URL, resource access right data, and key data, and the RDS stores the key data used by the RPS, the RDS verifying that the resource access right data has not changed from establishment by the RPS using the key data.

50. A system as claimed in claim 47 wherein the key data includes a key and optionally at least one of:

1) a second URL identifying the RPS;

2) start date/time data identifying a date and time at which a key is valid;

3) end date/time data identifying a date and time at which a key becomes invalid;

4) lifespan data indicating a period of time over which the key is valid;

5) key index data identifying the key from among a plurality of different keys;

6) hash identifier data indicating to the RDS a hash algorithm to be performed to generate the hash data;

7) encryption data indicating an encryption model and/or algorithm used to encrypt and decrypt resource access right data; and/or

8) format fields data indicating the number of fields in the signal requesting access to the resource.

51. A server storing a secure universal resource locator (URL) generator module executable by the server to generate a URL having secure resource access right data defining restriction(s) on a web access device (WAD) and/or user thereof to access a resource indicated by the secure URL, the resource access right data secured by the server so that modification of the resource access right data can be detected.

52. A server as claimed in claim 51 wherein the server stores a secure content key database having key data, and the server executes the secure URL generator module to secure the resource access right data with the key data.

53. A server as claimed in claim 51 wherein the server appends the key data to an Internet protocol (IP) address of the WAD requesting the web page document from the server, and hashes the key data and the IP address to generate hash data, the hash data combined with the URL and resource access right data to generate the secure URL.

54. A server as claimed in claim 51 wherein the server uses the key data to encrypt the resource access right data and combines the encrypted resource access right data with the URL to produce the secure URL.

55. A server as claimed in claim 51 wherein the server comprises a resource access right database storing the resource access right data.

56. A server as claimed in claim 51 wherein the server comprises an access right enforcer module, the server executing the access right enforcer module to determine whether a resource is to be provided to another server in response to a request signal received from the other server via the Internet, the server executing a secure caching module to transmit the resource to the other server for distribution if the resource access right data indicates that the other server is authorized to access the resource, and the server preventing access to the other server if the resource access right data indicates the other server is not authorized to access the resource.

57. A server of a resource distribution subsystem (RDS) storing an access right enforcer module executable by the server, the server executing the access right enforcer module in response to a signal from a web access device (WAD) requesting access to a resource, the request signal having a universal resource locator (URL) with secure resource access right data, the server executing the access right enforcer module using resource access right data to determine whether the resource access right data has been modified after its establishment by a resource provider subsystem (RPS), the server preventing access to the resource if the resource access right data has been modified after its establishment, the server further executing a secure caching module if the resource access right data has not been modified to provide access to the resource if the WAD is determined by the server to have the right to access the resource based on the resource access right data, and the server blocking access to the resource if the WAD is determined not to have the right to access the resource.

58. A server as claimed in claim 57 wherein the request signal received by the server from the WAD includes an Internet protocol (IP) address, a universal resource locator (URL) indicating the location of the resource, and hash data, the server retrieving key data based on the IP address and/or URL, the server combining the key data with at least the IP address and/or URL, the server generating hash data based on the key data and IP address and/or URL, the server comparing the server-generated hash data with the hash data in the request signal, the server executing its secure caching module to provide access to the resource if the hash data matches, and the server blocking access to the resource if the hash data do not match.

59. A server as claimed in claim 57 wherein the server retrieves date/time data from a secure content key database stored therein, the date/time data indicating a period of time over which the key data is valid, the server recording the date and time of receiving the request signal at the server and comparing the date and time of receipt of the request signal with the date/time data to determine whether the key data is valid, the server permitting further processing of the request signal if the comparison indicates the key data is valid, and the server terminating further processing of the request signal if the date/time data indicates the key data is not valid.

60. A server as claimed in claim 59 wherein the server further retrieves from the secure content key database life span data that the server uses in conjunction with the date/time data to determine the period of time over which the key is valid so that date and time of receiving the request signal at the server can be compared by the server with the date/time data and lifespan data to determine whether the key is valid.